RECEIVED
CENTRAL FAX CENTER
JUN 19 2007

REMARKS

Claims 21 and 31 are amended. Claims 21-31, as amended, remain in the application. No new matter is added by the amendments to the Claims.

The Rejections:

In the Office Action dated March 19, 2007, the Examiner rejected Claims 21-31 under 35 U.S.C. 103(a) as being unpatentable over Kanevsky, et al. (US 6,421,453) and further in view of An, et al. (US 6,715,073).

As per Claim 21, the Examiner stated that Kanevsky discloses a method of initiating a procedure within a building comprising the steps of:

a. defining at least one initiating event for the procedure; [col. 1, lines 49-52 and col. 8, lines 5-12]

b. defining at least one requirement for the procedure; [col. 1, lines 52-56 and col. 12, lines 37-48]

c. defining at least one person to be authorized [col. 1, lines 57-63] to perform the procedure; [col. 5, lines 12-30 and col. 12, lines 37-40]

d. detecting the occurrence of the at least one initiating event; [col. 1, lines 65-67 and col. 9, lines 1-3]

e. generating a virtual key [col. 3, lines 29-67 col. 17, lines 57-58] for the at least one based on the at least one requirement detecting the occurrence of the at least one initiating event and prior to the at least one person arriving at the building; [col. 3, lines 30-32 and col. 17, lines 5-7]

f. transmitting virtual key to the at least one person; [col. 17, lines 5-7 and 59-60]

g. detecting use of the virtual key; [col. 9, lines 64-66 and col. 16, lines 64-66]

h. checking the validity of the virtual key; and [col. 5, lines 39-43 and col. 12, lines 42-48]

i. initiating said procedure within the building if the validity check is positive. [col. 4, lines 61-66 and col. 15, lines 40-46]

j. performing said steps a. through i. in an access control computer system associated with the building. [col. 3, lines 28-30 and col. 4, lines 61-63]

According to the Examiner, Kanevsky discloses initiating event, which can broadly be given as the presence of a user attempting to access a facility, building, or vehicle/boat (col. 13, lines 54-60). A requirement broadly interprets as any kind of security tasks that involves authorization or verification process necessary for (the procedure) gaining access to the facility (initiating event). Kanevsky discloses the claimed requirement refers to security tasks or user recognition (classification, identification, and verification) where this may involve interacting with the system to gain access (col. 1, lines 35-36 and 49-51). In addition, Kanevsky includes a password verification as claimed the requirement for the procedure (to access) to the facility (initiating event) by using a gesture pin or password (virtual key) *suggesting proof of* possession *in order to gain access* (col. 5, lines 3-10 and *40*-42). Kanevsky discloses the password includes a sequence of intentionally performed gestures is referred to as gesture pins (col. 5, lines 5-10 and 38-42). The virtual key can obviously be Kanevsky's password (or gesture pin) that is used to verify the person or user to gain access to the building or facilities (col. 5, lines 40-43 and col. 8, lines 23-40). Kanevsky discloses *the* passwords *(gesture pins) are* generated during *an* enrollment session where during enrollment session, gesture pins may be either predefined or provided to a user (col. 17, lines 5-7). Therefore, the gesture pin is transmitted to the user for use to access the facility/service prompting checking the validity of the gesture pin (col. 15, lines 41-47 and 18, lines 8-24). So depending on the security task(s) involved and the results of the user evaluation, the user is either granted/denied access to a service/facility or confirmed/denied with respect to ownership of an item (proof of possession, or information pertaining to the user's biometrics will be stored in a user database for different applications (col. 8, lines 5-12 and col. 1 2, lines 37-48). However, Kanevsky does not specifically disclose a password refers to a virtual key.

Hence, An, et al. is brought forth to teach a virtual key can also be considered as a password. An teaches organizations controls access for customers or users by registering user identification and passwords. That the password is a virtual key that authenticates a user (col. 1, lines 43-48 and col. 2, lines 4-10). Thus, it would have been obvious for a person of ordinary

skills in the art at the time of the invention to combine the teaching of the gesture pin or password as taught by Kanevsky with the teaching of a virtual key is also referred as a password as taught by An because both virtual keys and passwords has a common function which is for use to authenticate/authorize a user to gain access (to facilities/services).

As per Claim 22, the Examiner stated see An on col. 1, lines 64-col. 2, line 1; discusses a step of assigning an encrypted code to the virtual key.

As per Claim 23, the Examiner stated see An on col. 2, lines 5-12; discusses the steps of adding a signature to the virtual key and identifying a recipient of the transmitted virtual key by the signature.

As per Claim 24, the Examiner stated see Kanevsky on col. 1, lines 49-55; discusses defining different procedures for different initiating events.

As per Claim 25, the Examiner stated see Kanevsky on col. 13, lines 59-62 and col. 29-53 discusses defining different requirements for different procedures.

As per Claim 26 see Kanevsky on col. 9, lines 25-27 and An on col. 1, lines 64-col. 2, line 12; discusses transmitting different virtual keys to said person for different initiating events.

As per Claim 27, the Examiner stated see Kanevsky on col. 17, lines 20-30 discusses storing said virtual key partially or completely.

As per Claim 28, the Examiner stated see Kanevsky on col. 17, lines 20-30; discusses the steps of identifying the at least one person with biometrics characteristics.

As per Claim 29: the Examiner stated method according to Claim 21, further comprising at least one of the steps of:

initiating a control procedure of an elevator in the building;

initiating a medical assistance procedure;

initiating a building cleaning procedure; and initiating a guest reception procedure.

The Examiner commented that Kanevsky discloses classification involves the differentiation of multiple individuals attempting to interact with the system and a purpose of identifying the individuals from their respective commands (col.1, lines 49-58 and col.5, lines 3-17). Kanevsky discusses that it is desirable to implement an extension of the identification task where the individuals attempting to interface with the computer are ranked so that a higher ranking

individual (i.e. supervisor) is allowed access over a lower ranked individual (i.e. data entry person) (col. 1, line 65- col. 2, line 1). Further, Kanevsky discloses an apparatus/procedure for obtaining access to a computer/facility/service via the utilization of gesture pins (col. 15, lines 29-32). Thus, it would have been obvious the computer/facility/service is referring to initiating a variety of procedures (i.e. an elevator in a building, medical assistance, building cleaning procedure or guest reception) that includes security tasks for different users to access to different services/facilities.

As per Claim 30, the Examiner states see col. 31, lines 63-64; discusses the step of transmitting the virtual key using wireless devices.

As per Claim 31, the Examiner stated a method of initiating a procedure within a building comprising the steps of:

a. defining at least one initiating event for the procedure; [col. 1, lines 49-52 and col. 8, lines 5-12]

b. defining at least one of a security requirement and an availability requirement for the procedure; [col. 1, lines 52-56 and col. 12, lines 37-48]

c. defining at least one person to be authorized [col.1, lines 57-63] to perform the procedure; [col. 5, lines 12-30 and col. 12, lines 37-40]

d. detecting the occurrence of the at least one initiating event; [col. 1, lines 65-67 and col. 9, lines 1-3; detecting the occurrence is when the person comes to the interacting system or interface area (col. 1, lines 16-22)]

e. generating a virtual key [col. 3, lines 29-67 col. 17, lines 57-58] for the at least one based on the at least one requirement detecting the occurrence of the at least one initiating event and prior to the at least one person arriving at the building; [col. 3, lines 30-32 and col. 17, lines 5-7]

f. transmitting virtual key to the at least one person; [col. 17, lines 5-7 and 59-60]

a. detecting use of the virtual key; [col. 9, lines 64-66 and col. 16, lines 64-66]

g. checking the validity of the virtual key; and [col. 5, lines 39-43 and col. 12, lines 42-48]

h. initiating said procedure within the building if the validity check is positive. [col. 4, lines 61-66 and col. 15, lines 40-46]

i. performing said steps a. through i. in an access control computer system associated with the building. [col. 3, lines 28-30 and col. 4, lines 61-63]

Kanevsky discloses initiating event, which can broadly be given as the presence of a user attempting to access a facility, building, or vehicle/boat (col. 13, lines 54-60). A requirement broadly interprets as any kind of security tasks that involves authorization or verification process necessary for (the procedure) gaining access to the facility (initiating event). Kanevsky discloses the claimed requirement refers to security tasks or user recognition (classification, identification, and verification) where this may involve interacting with the system to gain access (col. 1, lines 35-36 and 49-51). In addition, Kanevsky includes a password verification as claimed the requirement for the procedure (to access) to the facility (initiating event) by using a gesture pin or password (virtual key) suggesting proof of possession in order to gain access (col. 5, lines 3-10 and 40-42). Kanevsky discloses the password includes a sequence of intentionally performed gestures is referred to as gesture pins (col. 5, lines 5-10 and 38-42). The virtual key can obviously be Kanevsky's password (or gesture pin) that is used to verify the person or user to gain access to the building or facilities (col. 5, lines 40-43 and col. 8, lines 23-40). Kanevsky discloses the passwords (gesture pins) are generated during an enrollment session where during enrollment session, gesture pins may be either predefined or provided to a user (col. 17, lines 5-7). Therefore, the gesture pin is transmitted to the user for use to access the facility/service prompting checking the validity of the gesture pin (col. 15, lines 41-47 and 18, lines 8-24). So depending on the security task(s) involved and the results of the user evaluation, the user is either granted/denied access to a service/facility or confirmed/denied with respect to ownership of an item (proof of possession, or information pertaining to the user's biometrics will be stored in a user database for different applications (col. 8, lines 5-12 and col. 12, lines 37-48). However, Kanevsky does not specifically disclose a password refers to a virtual key.

Hence, An, et al. is brought forth to teach a virtual key can also be considered as a password. An teaches organizations controls access for customers or users by registering user identification and passwords. That the password is a virtual key that authenticates a user (col. 1,

RECEIVED
CENTRAL FAX CENTER
JUN 19 2007

lines 43-48 and col. 2, lines 4-10). Thus, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of the gesture pin or password as taught by Kanevsky with the teaching of a virtual key is also referred as a password as taught by An because both virtual keys and passwords has a common function which is for use to authenticate/authorize a user to gain access (to facilities/services).

Applicants' Response:

On form PTOL-326, the Examiner indicated that the action is FINAL. However, nowhere in the Detailed Action does the Examiner state that the action is final. In accordance with MPEP § 706.07(h) VIII. FIRST ACTION FINAL AFTER FILING AN RCE, the action immediately subsequent to the filing of an RCE with a submission and fee under 37 CFR 1.114 may be made final only if the conditions set forth in MPEP § 706.07(b) for making a first action final in a continuing application are met and form paragraph 7.42.09 should be used if it is appropriate to make the first action after the filing of the RCE final. Accordingly, Applicants request that the Examiner confirm that the action is not final.

The method according to the present invention generates a virtual key in response to the detection of the occurrence of a certain event. (Page 2, Lines 22-23) The person to whom the key is communicated is made to depend on the type of event. (Page 3, Lines 1-2) The event can be an emergency call, an order, a request such as for a cleaning service, an invitation, or a periodically recurring event such as, for example, monitoring a condition, or a service. (Page 3, Lines 23-25) The type of event determines what requirements are specified for the key such as security and availability. (Page 3, Lines 26 to Page 4, Line 3)

It is through the event that the person to be authorized is defined. (Page 4, Line 5) The person is defined in a processing step "Specify Person to be Authorized" **13**. (Page 4, Lines 8-9) As shown in the drawing of the flowchart for the method according to the present invention, the event occurs at the starting point **11** which is before the step **13** of specifying the person to be authorized.

Thus, Claims 21-31 define a method in which the virtual key is generated only when the initiating event occurs and is detected. Only then is the virtual key generated and transmitted to

an authorized person. Therefore, Claims 21-31 define a method whereby an authorized person can only access a building if the initiating event has indeed occurred. Examples, of such initiating events are set forth on page 3 of Applicants' specification at lines 23-25.

Applicants step a. of Claims 21 and 31 is amended to recite "defining at least one initiating event for the procedure which event does not involve a person arriving at the building". Applicants step e. of Claims 21 and 31 recites "generating a virtual key for the at least one person based on the at least one requirement upon detecting the occurrence of the at least one initiating event and prior to the at least one person arriving at the building".

According to the Examiner, Kanevsky discloses an initiating event, which can broadly be given as the presence of a user attempting to access a facility, building, or vehicle/boat (col. 13, lines 54-60). A requirement broadly interprets as any kind of security tasks that involves authorization or verification process necessary for (the procedure) gaining access to the facility (initiating event). Kanevsky discloses the claimed requirement refers to security tasks or user recognition (classification, identification, and verification) where this may involve interacting with the system to gain access (col. 1, lines 35-36 and 49-51).

Clearly the Examiner equates the Kanevsky computer user arriving at the computer for an enrollment session to perform the intentional gesture sequence with Applicants' at least one person arriving at the building. Just as clearly, Applicants' initiating event occurs before the at least one user arrives at the building

Applicants believe that this amendment distinguishes the claimed method from the Kanevsky patent that shows a method and a system for user recognition employing behavioral passwords to access a computer, a service, or a facility. According to the Examiner, the initiating event is the presence of a computer user and the "gesture pin" is the virtual key that is generated and stored before the "initiating event". This is the opposite order of Applicants' steps d. and e.

The Examiner made of record on Form PTO-892, but did not discuss, references to Coppersmith et al. (US5796827), Simon et al. (US6195648), O'Donnell et al. (US7117529) and Flickner et al. (US6282553). Applicants reviewed these references and found them to be no more pertinent than the prior art relied upon by the Examiner in the rejections.

In view of the amendments to the claims and the above arguments, Applicants believe that the claims of record now define patentable subject matter over the art of record. Accordingly, an early Notice of Allowance is respectfully requested.